CONTROLES - SISTEMA VOTO POR BOLETA ÚNICA ELECTRÓNICA

Proyecto de Cursado: Auditoria de Sistemas

Universidad Nacional Del Sur

Segundo Cuatrimestre de 2019

Grupo 1

FRITZ Jonathan Alberto – LU: 99761

FUENTES Luciano Ezequiel – LU: 107570

PANDOLFI Manuel – LU: 108597

Contenido

1. Introducción

El propósito de este documento es establecer las bases sobre las cuales vamos a actuar como auditores externos del sistema de voto electrónico, Boleta Única Electrónica, desarrollado por el Grupo MSA, desarrollando los puntos más importantes, críticos y de mayor importancia.

El proceso de auditoría se llevará a cabo siguiendo las normas y lineamientos propuestos por los estándares de ISACA. Dichas normas requieren una planificación y ejecución de las tareas con el objetivo de obtener seguridad sobre el sistema a auditar y también que cumplan con las leyes y regulaciones establecidas para el proceso de sufragio correspondiente. Por supuesto, como auditores certificados, desempeñamos nuestras funciones bajo el código de ética ISACA.

En este contexto, se realizará una auditoría sobre los procesos críticos y con el objetivo de establecer debilidades de control, generando una opinión de auditoría correspondiente y dando algunas recomendaciones las cuales permitirán mejorar la calidad del sistema.

1.1. Roles

En calidad de Auditores Externos a la empresa Grupo MSA y al Gobierno de la Ciudad Autónoma de Buenos Aires, el equipo de auditoría integrado por un staff de profesionales llevará a cabo el proceso de auditoría.

1.2. Metas

Se han dispuesto las siguientes metas:

- Realizar un análisis completo del sistema de voto electrónico, sus problemas y sus fallas actuales.
- Evaluar la integridad de la información que se obtiene luego de realizada la tarea.
- Supervisar los controles actuales y proponer nuevos en caso de que hagan falta.
- Evaluar la eficiencia del software utilizado, así como también de las terminales.
- Supervisar los requerimientos legales que regulan la actividad y su correcto cumplimiento.
- Evaluar, controlar y planificar sistemas de controles internos apropiados para proporcionar la adecuada seguridad informática que amerita el proceso completo.

1.3. Alcance de la tarea Realizada

El alcance se define para el Sistema de Voto por Boleta Única Electrónica. Esto implica todos sus componentes, tanto de hardware como también de software. Se realizará una evaluación completa del sistema, incluyendo aspectos legales y de normativa nacional, así como también la calidad de los procesos utilizados. Por último, se evaluarán los beneficios y debilidades del mismo en comparación con el sistema tradicional.

1.4. Objetivo Perseguido

Generar un informe en el cual se analice si el Sistema de Voto por Boleta Única Electrónica presenta las distintas características esenciales y necesarias que debe tener un sistema de software tan sensible, incluyendo confiabilidad, seguridad e integridad de los datos del sufragio. A su vez, se busca que el sistema permita:

- Realizar una función correcta del fin para el cual fue creado. Esto implica que el sistema que integra funcione de manera correcta y tanto la computación de los votos como la generación de los resultados, ambas sean íntegras en toda su dimensión.
- Que las personas puedan realizar el sufragio de manera sencilla, logrando así una opción viable para el reemplazo (o al menos esa es la intención) del sistema convencional de voto tradicional.
- Permitir que las personas con distintas discapacidades motrices o de cualquier otro tipo, puedan realizar el sufragio de manera fácil, sin que su discapacidad implique motivo de dificultad al realizar dicha acción.
- Reducir los costos insumidos en el sistema tradicional y por el cual se busca avanzar sobre esta modalidad de voto.

1.5. Requerimientos de Auditoría

Para el desarrollo de la presente auditoría, se solicitaron diversos documentos tanto a la empresa que desarrolló el sistema como al Gobierno de la Ciudad de Buenos Aires que lo implementará. Por otro lado, se recolectó información desde sitios oficiales en la web:

- Documento: “Voto electrónico: Los riesgos de una ilusión”.
- Código fuente.
- Ficha técnica del sistema de Boleta Única Electrónica.
- Documentación pública del sistema.
- Material de difusión emitido para los usuarios del sistema de votación.
- Documento de análisis de requerimientos.
- Documento de arquitectura y diseño del sistema.
- Documento de pruebas pertinentes al sistema.
- Política de control interno de la empresa MSA.

1.6. Funciones a ser auditadas

A partir de la información que pudo ser recolectada, se auditó el conjunto de funciones que implica el proceso de sufragio, considerando desde la preparación e instalación de los equipos hasta el recuento final del escrutinio, pasando en el medio por la emisión propia del voto, interacción de distintos usuarios con el hardware y software, la transmisión de resultados y la seguridad e integridad de los datos.

1.7. Tiempo insumido en las tareas

Para la realización de la presente auditoría de Sistema Voto por Boleta Única Electrónica se dedicaron 40 horas.

1.8. Staff de Auditoría

El equipo de auditoría está conformado por auditores CISA, por lo que actuarán bajó el código de ética correspondiente.

- **Fuentes Luciano Ezequiel - Auditor líder del equipo de auditoría:** Es el encargado de definir los recursos necesarios y la evidencia que se desea recolectar. Acordar reuniones con la gerencia de Grupo MSA, autoridades del gobierno de la Ciudad Autónoma de Buenos Aires y con el equipo de auditoría. Dirigir el resto del proceso: evaluación de los riesgos, de la evidencia, generación de reportes y la comunicación de los resultados.
- **Fritz Jonathan - IT Senior:** Asistente en la evaluación de los riesgos, de la evidencia, generación de reportes y comunicación de los resultados.
- **Pandolfi Manuel - Auditor experto en seguridad informática:** Es el encargado de evaluar la efectividad de los equipos de hardware y software en la confidencialidad, integridad y disponibilidad de los datos.

2. Comunicación de Resultados

2.1. Debilidades Encontradas

Se han encontrado una serie de debilidades en el sistema de voto electrónico, las cuales se detallan a continuación. Para cada una se describe el problema, su riesgo asociado, la valuación del mismo y la evidencia recolectada. Además, se propone una posible solución de forma de mitigar el riesgo.

2.1.1. Equipos Desprotegidos

Descripción: No existen procedimientos eficaces para la protección de los equipos usados para realizar el proceso de voto electrónico.

Riesgo Asociado: Es factible cualquier manipulación maliciosa de los equipos debido a dicha desprotección.

Valuación del Riesgo: Medio.

Evidencia: El historial en cuanto a mecanismos de seguridad y protección de equipos ha probado que los mismos son fácilmente violables y vulnerables.

Posible solución: Definir políticas y establecer procedimientos eficaces para la protección de los equipos encargados de realizar la operatoria de voto electrónico.

2.1.2. Falta de procedimientos de validación de resultados

Descripción: No se han establecido procedimientos de control que permitan validar los resultados del escrutinio provisorio realizado por medios electrónicos.

Riesgo Asociado: Aumenta la chance de que los resultados no sean aceptados por no haber controles adecuados. No se conoce con certeza si el sistema funcionó correctamente.

Valuación del Riesgo: Alto.

Evidencia: Se ha evidenciado la falta de dichos procedimientos, lo cual genera cierto tipo de incertidumbre y poca claridad sobre los resultados obtenidos.

Posible Solución: Se deberían definir de antemano (planificación), actividades y pruebas que permitan realizar simulaciones y de esa manera poder asegurar que los resultados obtenidos por el sistema sean válidos.

2.1.3. Falta de información hacia el público general

Descripción: El Tribunal Superior de Justicia de la Ciudad de Buenos Aires, la cual actúa como autoridad de aplicación de la norma legal, no ha puesto información accesible y a disposición de los ciudadanos, partidos políticos y cualquier otro interesado respecto al asunto.

Riesgo Asociado: El sistema incumple principios básicos y fundamentales, así como la norma legal que lo habilita.

Valuación del Riesgo: Alto.

Evidencia: No se han encontrado documentos que informen al público y comunidad sobre el manejo del sistema y su funcionamiento. Esto incumple lo establecido por la Ley n° 4894.

Posible Solución: Los interesados en hacer funcionar el procedimiento de la correcta manera (la Ciudad de Buenos Aires en este caso), debería, en primer lugar, poner personal a disposición para el seguimiento del cumplimiento de las disposiciones legales en lo que a la implementación del sistema se refiere. Por otra parte, se requiere de la documentación respectiva, la cual debe de avalar dicho seguimiento.

2.1.4. Complejidad en la cadena de suministro

Descripción: Estamos ante la presencia de un sistema el cual involucra una secuencia de pasos críticos. Cualquier falla en alguno de ellos implica un error crítico en el siguiente. Cada paso es fundamental para el proceso electoral.
Riesgo Asociado: Una falla accidental o inducida, se propaga hasta el resultado final, afectando el proceso electoral por completo.

Valuación del Riesgo: Alto.

Evidencia: Marcada insuficiencia en los procedimientos establecidos por la autoridad electoral, la cual eleva los riesgos de que una falla sea posible.

Posible Solución: Realizar una adecuada evaluación de los posibles riesgos en la cadena de suministro, y en base a ella definir planes de seguridad física y/o electrónica para cada uno de los pasos y de esta manera reducir la probabilidad de ocurrencia de fallos.

2.1.5. Falta de compresión del proceso electoral

Descripción: El proceso electoral debe ser comprendido y entendido por todos sus involucrados y no debe de tener inconsistencias de ningún tipo. En particular, las personas con derecho a sufragio activo deben de saber bien cómo funciona de manera que puedan creer en la veracidad del mismo. Cada vez que existen sistemas informatizados, una parte del proceso pasa a ser tareas automáticas, las cuales muchas veces quedan definidas en términos de actores poco claros. A su vez el rol de los técnicos no está del todo claro.

Riesgo Asociado: El reemplazo de una parte significativa del proceso electoral por un procedimiento automático cuyo funcionamiento no se conoce en su totalidad y su manipulación, es relativamente viable a su vez genera pocas garantías de compresión plena. Incluso cuando estas acciones son llevadas a cabo en público y de manera abierta.

Valuación del Riesgo: Alto.

Evidencia: Se han evidenciado en circunstancias similares (misma empresa, misma tarea, mismo rol) el desarrollo de operaciones críticas sin la supervisión que dichas tareas ameritan. Particularmente, los técnicos ´poseen cierta independencia, lo cual los dota de un rol bastante autónomo y el cual no deberían de tenerlo.

Posible Solución: Para aumentar la transparencia y generar mayor confianza (confianza real) hacia todos los participantes e involucrados es importante que el personal esté bien capacitado y a su vez se creen fuertes políticas de control para que ninguno tenga más acceso del debido y que cada uno asuma la responsabilidad que le concierne.

2.1.6. Replicación de software

Descripción: Los efectos de una intervención maliciosa o una falla accidental se multiplican a todos los lugares de votación de manera muy eficiente. A su vez, la superficie de ataque se expande enormemente. El número de partes en colusión requeridas para una intervención maliciosa se reduce considerablemente, basta un solo programador malintencionado para introducir código que afecte la veracidad del resultado de una elección.

Riesgo Asociado: Es factible la manipulación de resultados electorales, dando como consecuencia un rechazo de los mismos ya que sería muy poco posible la refutación de dichas acusaciones de manipulación. Todo esto genera una desconfianza absoluta en el sistema electoral.

Valuación del Riesgo: Alto.

Evidencia: En el proceso electoral actual se requiere que el fraude sea realizado en cada uno de los puntos de votación, lo cual es imposible ya que la descentralización es grande. Incluso cuando fuere posible, el impacto sería menor. Por otra parte, en sistemas de voto electrónico, el hecho de que cada terminal esté programada de la misma forma permite que un solo código malicioso pueda expandirse al resto sin mucha dificultad. Esto “invita” oportunamente a una posible manipulación a gran escala.

Posible Solución: Se debe de realizar un adecuado análisis de riesgos orientados a la manipulación de los datos generados y obtenidos, consultando a los profesionales adecuados (seguridad informática), de forma de prever buenos mecanismos de protección frente a adulteración y modificación de los datos.

2.1.7. Votos que no reflejan la intención del votante

Descripción: Es posible que los votantes que no estén familiarizados con el sistema de voto emitan algo que no refleje sus preferencias. La asistencia a los votantes con discapacidades puede resultar confusa, errónea o insuficiente o que las interfaces utilizadas generen inconvenientes para personas que anteriormente emitían su voto sin dificultad alguna y ahora presenten problemas para hacerlo.

Riesgo Asociado: Los votos emitidos por algunas personas no reflejan sus preferencias ni su intención real.

Valuación del Riesgo: Medio.

Evidencia: No se han probado de manera rigurosa los sistemas de usabilidad, generando inconvenientes. De hecho, en el mundo no hay pruebas científicas sobre usabilidad en este tipo de sistemas. No está probada la interacción de los votantes (tanto personas con alguna dificultad como personas sin dificultades).

Posible Solución: Definir planes de validación del sistema para pruebas de usabilidad. Se deben de evaluar los distintos perfiles de usuario, realizar pruebas, y luego ajustar las interfaces de acuerdo a los resultados que arrojen dichas pruebas.

2.1.8. Baja calidad en la impresión de boletas

Descripción: La calidad de impresión de las boletas que el sistema brinda no es de una calidad estándar o aceptable, generando malestar y desconfianza en los votantes.

Riesgo Asociado: Aparición de malestar y desconfianza en los votantes que utilizan el sistema

Valuación del Riesgo: Medio.

Evidencia: Se ha detectado en pruebas de prototipo realizadas con anterioridad que la impresión de las boletas carece de buena calidad.

Posible Solución: Utilizar un módulo de impresión adecuado para la impresión de las boletas. Teniendo en cuenta el ahorro monetario que genera el uso del sistema, invertir en calidad de impresión (teniendo en cuenta que la cantidad será menor), serviría para mitigar el problema.

2.1.9. Ausencia de verificación de versiones en el hardware y software

Descripción: No se han establecido mecanismos que aseguren que las versiones de software y hardware a utilizar se correspondan con las últimas y las que fueron previamente verificadas.

Riesgo Asociado: El software o hardware podría llegar a incluir fallas, lo cual podría generaría un problema gravísimo durante la votación.

Valuación del Riesgo: Medio.

Evidencia: No existe mecanismo formal que asegure que la versión de hardware y software que fue entregada, es la que se verificó de manera correcta y está libre de errores.

Posible Solución: Agregar mecanismos de trazabilidad entre los distintos componentes del sistema, los cuales permitan identificar cada módulo, cada programa y cada componente de hardware, para luego trazar una verificación y validación real con lo que los documentos han establecido de antemano.

2.1.10. Dependencia eléctrica

Descripción: Las terminales funcionan con electricidad, lo cual indefectiblemente se convierte en una debilidad. Se requiere de cierta estabilidad eléctrica y a su vez que dicha electricidad llegue a cada uno de los equipos.

Riesgo Asociado: Un corte de luz (podría llegar a ser voluntario) generaría una parada obligatoria en el escrutinio. Tanto durante la votación como luego de ella.

Valuación del Riesgo: Medio.

Evidencia: Es posible que se quiera arruinar o invalidar una elección y este sería un medio viable.

Posible Solución: Se debería de contemplar el uso de generadores propios de electricidad. Esto a su vez es en parte un cuello de botella debido a que se necesitaría uno para cada escuela, que supla cada mesa y cada lugar de votación.

2.1.11. Falta de controles generales

Descripción: La presión por cierta parte del sector público genera que muchas de las deficiencias nombradas pasen por alto debido, generando así cierta "incertidumbre" y librando al azar (o a muy pocas manos) responsabilidades grandísimas las cuales deberían de estar contempladas desde la planificación.

Riesgo Asociado: Responsabilidades en manos de pocos, lo cual tiene como consecuencia falta de confianza del público en general.

Valuación del Riesgo: Medio.

Evidencia: Se han evidenciado ciertos sectores los cuales están muy a favor de la implementación del voto electrónico, los cuales muchas veces por una cuestión de querer implementación rápida pasan por alto los controles debidos para un correcto uso.

Posible Solución: Aumentar los controles en las etapas de planificación y realizar procedimientos de verificación en cada paso.

2.1.12. Logística y distribución del hardware

Descripción: El hardware podría no llegar a tiempo y/o no llegar nunca a ciertos sectores, por falta de infraestructura o bien por falta de logística que permita que llegue finalmente a cada lugar donde se lo necesita.

Riesgo Asociado: Los votantes no podrían realizar su voto, dejando nula su intención por fuerzas mayores.

Valuación del Riesgo: Bajo.

Evidencia: Se ha evidenciado cierta falta de garantías para proveer de los terminales a ciertos sectores.

Posible Solución: Asegurar con controles que la disponibilidad de dichos elementos esté asegurada.

3. Conclusión

3.1. Opinión de Auditoría

Luego del proceso de auditoría realizado sobre el sistema de Boleta Única Electrónica desarrollado por el Grupo MSA, el equipo de auditoría llegó a la conclusión que la documentación brindada por la empresa y por el gobierno de la Ciudad Autónoma de Buenos Aires es insuficiente. A pesar de que tanto la empresa y el gobierno se mostraron predispuestos a otorgar toda la información necesaria para realizar la auditoría, dichas fuentes de datos son de carácter subjetiva por lo cual no es correcto basar los resultados de la auditoría en las mismas. Ésta carece de información sobre ciertas funcionalidades implementadas, tecnologías utilizadas, decisiones de diseños y pruebas de código. Dichos aspectos encontrados en el proceso llevaron al equipo a estar limitados en el alcance del trabajo realizado. Por dicha razón, no es posible poder emitir opinión respecto a los mismos.

Por último, podemos decir que el sistema de Boleta Única Electrónica presenta graves fallas en el aseguramiento de la calidad. Esto involucra cuestiones como la integridad de los datos, usabilidad, seguridad y robustez. La falta de documentación referida al proceso de desarrollo también son parte de las deficiencias del sistema, impidiendo así un desarrollo de software de calidad.

Por otra parte, creemos que es posible lograr un Sistema de Voto Electrónico viable y útil, el cual permita una reducción significativa de los costos y facilidad en muchos aspectos importantes. Sin embargo, para ello hace falta que los controles sean los adecuados y estén presenten en cada etapa, en cada actor y en cada circunstancia del proceso, logrando así un sistema viable y en el cual las personas confíen en él. Por ello se necesita una integración de las partes y que cada uno se comprometa a cumplir con su rol, participación y control que le concierte a cada uno, logrando en forma conjunta que el sistema funcione correctamente.

3.2. Limitaciones del Alcance

No se pudo tener acceso a los siguientes documentos que eran parte del requerimiento inicial para realizar la auditoría:

- Código fuente.
- Documentos del proceso de desarrollo del sistema.
- Documentos del proceso de prueba del sistema.
- Proceso de seguimiento de la información luego de terminado el escrutinio.

El haber contado con esos recursos mencionados hubiera sido de gran utilidad para poder realizar un análisis más profundo dentro de la implementación de los equipos para votar. Una de las causas más significante por la cual el sistema de voto electrónico tiene baja credibilidad, se da ya que es un sistema que solo pocas personas saben cómo funciona internamente y cómo es que procesa los datos. Por lo tanto, que esta información siga sin estar accesible a la hora de realizar una auditoría profundiza esta

desconfianza. Distintos aspectos en relación a la seguridad del sistema podrían mitigarse en caso de conocer cómo es la implementación.